SPYWOLF

Security Audit Report

Completed on

April 28, 2023

OVERVIEW

This audit has been prepared for **XPEPE** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

XPEPE

PROJECT DESCRIPTION

According to their whitepaper:

XPepe is a novel cryptocurrency venture that merges SpaceX and PEPE to aid investors in reaching the moon once it becomes available for trading. While PEPE is well-known for its comedic value, XPEPE's appeal extends beyond that due to the advantages that this scheme offers. XPepe is a novel cryptocurrency venture that merges SpaceX and PEPE to aid investors in reaching the moon once it becomes available for trading. While PEPE is well-known for its comedic value, XPEPE's appeal extends beyond that due to the advantages that this scheme offers.

Release Date: Presale starts in April, 2023

Category: Meme token

CONTRACT INFO

Token Name
XPepe

Symbol
XPepe

Contract Address
0x28a7d9D9FF581e24765d9C1FA94238fC4b1f740a

Network
Binance Smart Chain

Language
Solidity

Deployment Date
Apr 26, 2023

Verified?
Yes

Total Supply
490,000,000,000,000

Status
Not launched

TAXES

Buy Tax
15%

Sell Tax
18%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	490000000000000 XPepe
Median Transfer Amount	490000000000000 XPepe
Average Transfer Amount	490000000000000 XPepe
First transfer date	2023-04-26
Last transfer date	2023-04-26
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2023-04-26 10:23:54 UTC
Created	2023-04-26 10:23:54 UTC
Create TX	0xfd02bd8371b5400499b0c8fa4a34f68b3916599980d7d5fb94b3cad76c7dc1ad
Creator	0x67b69912042a502de234e87c029ed07718c55f8c

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Owner can set reward proportion equal to buy/sell fees.
When the tokens reserved for rewards are equal to buy/sell fees, the contract will halt once it reaches the auto swap threshold. This is irreversible and will affect all users that are not excluded from fees. Any further sell interactions with the contract will halt.

```
function setFee(uint256 rewardsFee_, uint256 buyFee_, uint256 sellFee_) external onlyOwner {
    require(buyFee_ <= 20 && sellFee_ <= 20, "over tax");
    require(buyFee_ >= rewardsFee_ && sellFee_ >= rewardsFee_, "reward too big");
    rewardsFee = rewardsFee_;
    buyFee = buyFee_;
    sellFee = sellFee_;
}

function _transfer(address from, address to, uint256 amount) internal override {
.....................
if (
    canSwap &&
    !swapping &&
    from != uniswapV2Pair &&
    !_isExcludedFromFees[from] &&
    !_isExcludedFromFees[to]
) {
    swapping = true;

    uint256 marketingTokens = contractTokenBalance.sub(rewardAmount);
    swapAndSendToFee(marketingTokens);

    uint256 sellTokens = balanceOf(address(this));
    swapAndSendDividends(sellTokens);
    rewardAmount = 0;

    swapping = false;
}

if (takeFee) {
    uint256 fee = to == uniswapV2Pair ? sellFee:buyFee;
    uint256 feeAmount = amount.mul(fee).div(100);
    uint256 reward = amount.mul(rewardsFee).div(100);
    amount = amount.sub(feeAmount);
    super._transfer(from, address(this), feeAmount);
    rewardAmount = rewardAmount.add(reward);
}
.....................
}
```

- Recommendation:
  - Ensure that rewardFee state variable is always lower than buyFee and selFee state variables.

FOUND THREATS

⚠ Medium Risk

Owner can set buy/sell fee up to 20%.
Combined buy+sell = 40%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.
Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function setFee(uint256 rewardsFee_, uint256 buyFee_, uint256 sellFee_) external onlyOwner {
    require(buyFee_ <= 20 && sellFee_ <= 20, "over tax");
    require(buyFee_ >= rewardsFee_ && sellFee_ >= rewardsFee_, "reward too big");
    rewardsFee = rewardsFee_;
    buyFee = buyFee_;
    sellFee = sellFee_;
}
```

- Recommendation:
  - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.

FOUND THREATS

⚠ Medium Risk

Owner can change contract's autoswap threshold.
If swapTokensAtAmount state variable is set to very low number or 0 and the contract's token balance is 0, selling will fail for all users.

```
function setSwapTokensAtAmount(uint256 amount) external onlyOwner {
    swapTokensAtAmount = amount;
}

function _transfer(
    address from,
    address to,
    uint256 amount
) internal override {

.....................
uint256 contractTokenBalance = balanceOf(address(this));
bool canSwap = contractTokenBalance >= swapTokensAtAmount;

if (
    canSwap &&
    !swapping &&
    from != uniswapV2Pair &&
    !_isExcludedFromFees[from] &&
    !_isExcludedFromFees[to]
) {
    swapping = true;

    uint256 marketingTokens = contractTokenBalance.sub(rewardAmount);
    swapAndSendToFee(marketingTokens);

    uint256 sellTokens = balanceOf(address(this));
    swapAndSendDividends(sellTokens);
    rewardAmount = 0;

    swapping = false;
}
.....................
}
```

- Recommendation:
  - Ensure that swapTokensAtAmount state variable is always above 1 token (considering decimals) to avoid such behaviour.

Informational

There is max transaction of 1% of total supply applied in the first 20 blocks after token's launch.
After that period, no limitations are applied.
The owner cannot set max transaction limit later on.

```
constructor(address rewardToken_, address router_, address mkt_)
.....................
maxTransaction = totalSupply_.mul(1).div(100);
.....................
}
function _transfer(
address from,
address to,
uint256 amount
) internal override {

.....................
if (_isExcludedFromFees[from] || _isExcludedFromFees[to]) {
    takeFee = false;
} else {
    if (startBlock == 0 || block.number < (startBlock + 20)) {
        require(amount <= maxTransaction, "max transaction in first 60s");
    }
}
.....................
}
```

Owner can exclude address from fees.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function excludeFromFees(address account, bool excluded) public onlyOwner {
    require(
        _isExcludedFromFees[account] != excluded,
        "Account is already the value of 'excluded'"
    );
    _isExcludedFromFees[account] = excluded;

    emit ExcludeFromFees(account, excluded);
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

XPepe

GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner cannot set a transaction limit
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

There is no percent based information about the initial tokens distribution according to the project's whitepaper and/or website.

TOKENOMICS

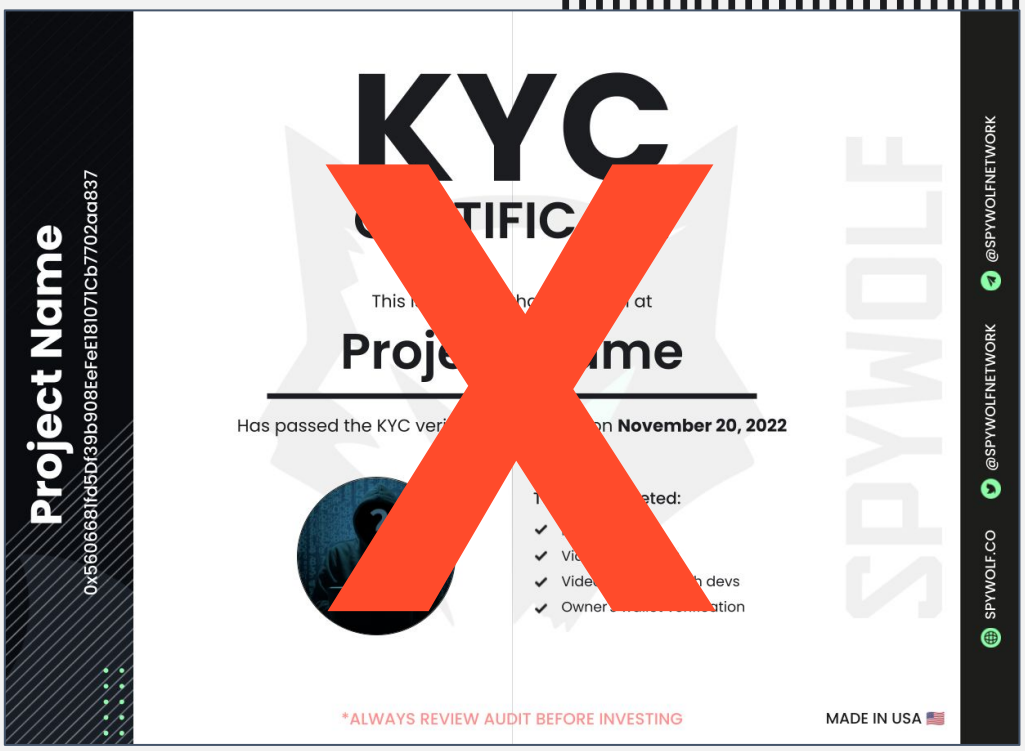
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://www.xpepe.xyz/

Domain Registry
https://namecheap.com

Domain Expiration
2024-04-27

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page design with appropriate color scheme.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
A bit short

Roadmap
Yes, goals set without time frames.

Mobile-friendly?
Yes

xpepe.xyz

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are new

Twitter

@XPepeMoon

- 7,,956 followers
- Brand new

Discord

- Not available

Telegram

@XPepe_Official

- 3 097 members
- Few active members
- No active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 500 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.